# DATA PRIVACY AND PROTECTION POLICY (SAMPLE)

Document Information

Title: Data Privacy and Protection Policy

Organization: ExampleCo, Inc. (fictional)

Version: 3.0

Effective Date: January 29, 2026

Last Review: January 29, 2026

Next Review: January 2027

Owner: Privacy & Security Office

Classification: Internal

Important Note

This is a sample internal policy provided for demonstration/training purposes. It is not legal advice and may not reflect your local legal requirements.

## TABLE OF CONTENTS

## 13. Training, Monitoring, and Compliance

## 14. Exceptions and Policy Maintenance

# 1. PURPOSE AND SCOPE

## 1.1 Purpose

This policy defines how ExampleCo, Inc. protects personal information collected, used, stored, and shared in the course of business.

## 1.2 Scope

This policy applies to:

- Employees, contractors, interns, and temporary staff
- Personal information processed by or on behalf of ExampleCo
- All systems, applications, services, and business processes that handle personal information

## 1.3 Applicable Requirements

ExampleCo aims to comply with applicable data protection and privacy requirements where it operates, including (as relevant):

### - EU/UK GDPR

- CCPA/CPRA (California)
- Other state, national, or sector-specific privacy requirements

Where requirements differ by jurisdiction, ExampleCo will follow the applicable local requirements and documented procedures.

# 2. DEFINITIONS

## 2.1 Personal Information / Personal Data

Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked (directly or indirectly) with an individual.

Examples include: name, email, phone, postal address, account identifiers, device identifiers, IP address, precise location, employment data, and certain cookies/analytics identifiers.

## 2.2 Sensitive Personal Information

Personal information that requires heightened protections due to its nature and potential impact if misused.

Examples may include: government identifiers, authentication secrets, precise geolocation, biometric identifiers, health information, and data revealing racial/ethnic origin, religious beliefs, union membership, sexual orientation, or similar categories where applicable.

### 2.3 Processing

Any operation on personal information, such as collecting, using, storing, sharing, analyzing, or deleting it.

### 2.4 Controller / Business

The party that determines why and how personal information is processed.

### 2.5 Processor / Service Provider

The party that processes personal information on behalf of the controller/business under a contract and documented instructions.

## 3. PRIVACY PRINCIPLES

ExampleCo follows these privacy principles:

### 3.1 Lawfulness and Transparency

- Use personal information only for legitimate, documented purposes
- Provide clear privacy notices and internal documentation describing use and sharing

### 3.2 Purpose Limitation

- Collect and use personal information for specific, explicit purposes
- Do not use personal information for materially different purposes without an appropriate legal basis and updated notices

### 3.3 Data Minimization

- Collect only what is needed for the stated purpose
- Prefer privacy-preserving defaults and limit access to what is required for the role

### 3.4 Accuracy

- Keep personal information reasonably accurate and up to date

- Provide processes for correction where appropriate

### 3.5 Storage Limitation

- Retain personal information only as long as required for business needs and legal obligations
- Apply documented retention schedules and deletion processes

### 3.6 Security and Confidentiality

- Implement appropriate administrative, technical, and physical controls
- Protect confidentiality, integrity, and availability of personal information

### 3.7 Accountability

- Maintain policies, procedures, and evidence of compliance
- Review and improve the privacy program regularly

## 4. ROLES AND RESPONSIBILITIES

### 4.1 Privacy Lead / Data Protection Officer (as applicable)

Responsibilities:
- Own the privacy program, privacy notices, and key procedures
- Advise on privacy impact assessments for higher-risk processing
- Serve as a point of contact for privacy requests and regulators (as required)

Contact (sample): privacy@example.com

### 4.2 Senior Leadership

- Ensure resourcing and governance for privacy and security
- Review material privacy risks and approve risk acceptances where required

### 4.3 Department Owners

- Ensure privacy-by-design in their processes and tools
- Identify privacy risks and engage the Privacy & Security Office early

### 4.4 IT / Security

- Implement and operate security controls (access, logging, encryption, backup)

- Support incident response and breach handling

### 4.5 All Personnel

- Follow this policy and related procedures
- Report suspected privacy or security incidents immediately
- Complete required training

## 5. LEGAL BASES AND NOTICES

### 5.1 Legal Basis (where required)

When required by applicable law, ExampleCo documents the legal basis for each processing activity (e.g., consent, contract, legal obligation, legitimate interests).

### 5.2 Consent

Where consent is used:

- Use clear opt-in choices and plain language
- Provide an easy way to withdraw consent
- Record what was consented to, when, and how

### 5.3 Privacy Notices

ExampleCo provides privacy notices appropriate to the context (website/app notice, employee notice, vendor/customer notices) describing:

- What data is collected and why
- How it is used and shared
- Retention periods
- Individual rights and how to exercise them
- Contact information

### 5.4 Legitimate Interests (where applicable)

When relying on legitimate interests, ExampleCo documents an assessment balancing business needs against individual rights.

## 6. INDIVIDUAL (DATA SUBJECT/CONSUMER) RIGHTS

ExampleCo supports requests to the extent required by applicable law. Rights vary by jurisdiction.

### 6.1 Access / Know

Individuals may request access to personal information held about them, subject to legal exceptions.

### 6.2 Correction

Individuals may request correction of inaccurate personal information.

### 6.3 Deletion

Individuals may request deletion of personal information, subject to legal exceptions (e.g., compliance obligations, security, legal claims).

### 6.4 Portability (where applicable)

For certain data and legal regimes, individuals may request a portable copy in a commonly used, machine-readable format.

### 6.5 Opt-Out of Sale/Sharing and Targeted Advertising (where applicable)

Where required (e.g., certain U.S. state laws), individuals may opt out of certain disclosures considered a “sale” or “sharing” and of targeted advertising.

### 6.6 Automated Decision-Making (where applicable)

If ExampleCo uses automated decision-making that has legal or similarly significant effects, individuals may have additional rights under applicable law.

### 6.7 Request Process

- Submit requests to: privacy@example.com
- ExampleCo may verify identity before fulfilling requests
- ExampleCo responds within applicable legal timeframes
- ExampleCo tracks requests for compliance and trend analysis

## 7. COLLECTION, USE, AND SHARING

### 7.1 Privacy by Design

- Evaluate privacy impacts early in projects (design/review)
- Use data minimization and access controls by default
- Perform a documented privacy impact assessment for higher-risk processing

### 7.2 Typical Categories of Collection

ExampleCo may process personal information relating to:

- Customers/users (account and support data)
- Website visitors (analytics/security logs)
- Employees/contractors (HR and payroll administration)
- Vendors/partners (business contact details)

### 7.3 Sharing

ExampleCo may share personal information with:

- Service providers/processors (e.g., hosting, support tools, analytics, payroll)
- Professional advisors (e.g., legal, audit) under confidentiality
- Authorities where required by law

Sharing is subject to contract, access controls, and the minimum necessary principle.

### 7.4 Children

ExampleCo services are not intended for children. If ExampleCo learns it collected personal information from a child contrary to applicable law, it will take appropriate steps to delete it.

## 8. RETENTION AND DELETION

### 8.1 Retention Schedule (Examples)

ExampleCo maintains a documented retention schedule. Common examples include:

Employee Records

- Employment records: employment term + up to 7 years (jurisdiction-dependent)
- Recruiting records (unsuccessful candidates): up to 1 year (or per local requirements)
- Payroll/tax records: per legal retention requirements

Customer/Support Records

- Account records: as long as the account is active
- Support tickets: typically 2–5 years

Security Logs

- Authentication and security logs: typically 90 days to 1 year depending on system and risk

### 8.2 Secure Deletion

ExampleCo securely deletes or de-identifies personal information when it is no longer required.

Secure disposal follows industry best practices (e.g., NIST SP 800-88 for media sanitization), and may include cryptographic erasure, secure overwriting where appropriate, and certified destruction for physical media.

### 8.3 Storage Locations

ExampleCo documents system data locations and environments (production/dev), and restricts access based on role and business need.

## 9. SECURITY CONTROLS

### 9.1 Access Controls

- Role-based access control (RBAC) and least privilege
- Multi-factor authentication (MFA) for administrative access and remote access
- Timely access revocation upon role change or termination

### 9.2 Encryption

- Encrypt data in transit using modern TLS
- Encrypt sensitive data at rest where feasible
- Manage keys using approved key management processes

### 9.3 Logging and Monitoring

- Security-relevant events are logged (authentication, admin actions, critical data access)
- Monitoring and alerting is implemented for suspicious activity

### 9.4 Physical and Administrative Controls

- Controlled access to offices and equipment
- Confidential materials handled and disposed of securely
- Background checks and confidentiality obligations where appropriate

### 9.5 Backups

- Backups are performed and tested according to system criticality
- Backup access is restricted and monitored

## 10. INTERNATIONAL TRANSFERS

Where personal information is transferred internationally, ExampleCo uses appropriate safeguards required by applicable law (e.g., SCCs, adequacy decisions) and documents the transfer mechanism.

## 11. VENDOR AND THIRD-PARTY MANAGEMENT

ExampleCo evaluates vendors that process personal information for security and privacy posture appropriate to the risk, and requires written terms covering:

- Processing instructions
- Confidentiality
- Security controls
- Subprocessors
- Breach notification
- Return/deletion at end of services

## 12. BREACH AND INCIDENT MANAGEMENT

### 11.1 Breach Definition

A personal data breach is a security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

### 12.2 Response Procedure

Upon discovering a suspected privacy/security incident:

### 1. Contain and preserve evidence

### 2. Assess impact (systems, data types, individuals affected)

### 3. Escalate to Security/Privacy on-call

### 4. Document actions and decisions

### 5. Remediate and prevent recurrence

### 12.3 Notification

ExampleCo notifies regulators and/or affected individuals when required by applicable law and contractual obligations. Timelines depend on jurisdiction and facts of the incident.

### 11.4 Breach Documentation

Document all breaches including:

- Facts of the breach
- Effects and consequences
- Remedial action taken
- Whether notification was required

## 13. TRAINING, MONITORING, AND COMPLIANCE

### 12.1 Mandatory Training

- All employees: Annual data protection training
- New hires: Training within first month
- High-risk roles: Specialized training
- Refresher training when policy changes significantly

### 12.2 Training Topics

- Data protection principles
- Individual rights
- Security best practices
- Breach reporting
- Role-specific responsibilities

### 12.3 Awareness Programs

- Regular privacy tips and reminders
- Privacy awareness campaigns
- Incident simulations and tabletop exercises
- Privacy champions program

### 13.1 Training

- Privacy and security training is required for all personnel
- Specialized training is provided for higher-risk roles (e.g., IT admins, customer support, HR)

### 13.2 Monitoring

ExampleCo monitors systems for security and compliance purposes consistent with applicable law and internal policy.

### 13.3 Documentation

ExampleCo maintains appropriate documentation (e.g., privacy notices, vendor agreements, risk assessments, incident records) to demonstrate compliance.

## 14. EXCEPTIONS AND POLICY MAINTENANCE

Any exception to this policy requires documented approval by the Privacy & Security Office and may require compensating controls.

## CONTACT

Privacy Requests (sample): privacy@example.com

Security Incidents (sample): security@example.com

Document ID: PRIV-POL-001

Approved by: Privacy & Security Office

Change History:

- v3.0 (Jan 2026): Rewrite for clarity, realism, and cross-jurisdiction use